CyberPatrol®

online protection pro

Online Protection User Manual

Contents

Overview **3**
Product Applications 3
Activating the Safety Center **4**
Activating Your Safety Center Account 4
Installing and Using the Scanner **7**
Scanner Installation 7
Using the Scanner 9
Safety Center *10*
Scanner Settings *11*
Safety Center Overview & Setup **13**
Safety Center Site Control Panel 13
Reports and Alerts 15
Summary Report *15*
Set Alert Notifications *15*
Instant Alerts *16*
Weekly or Monthly Reports *16*
Monitoring Info 17
Admin 18
Manage Computers *18*
Manage Licenses *19*
Account Information *19*
Advanced 20
Edit Shared Profiles *20*
Adding a User *21*
Applications **22**
Web Filtering 22
Block/Allow list *24*
Status Settings *25*
Time Management 25
SafeSearch 26
Sex Chat Alert 26
Harassment Alert 26
Custom Alert 26
Additional Information **29**
System Requirements 29
Uninstalling CyberPatrol Online Protection Pro 29
Web Filtering Categories and Definitions 30
Typically Blocked Categories *30*
Normally Allowed Categories *30*
Definitions and Terminology 32

Overview

CyberPatrol Online Protection Pro guards families against today's most common online threats. It is a service that uses a web site, the Safety Center, and a small software program, the Scanner, on any Windows PC with users you want to safeguard.

The Safety Center is used to manage computers, users, and protection levels for each computer and user. Once you have activated the Safety Center, you can manage any computer that has the Scanner installed. The number of computers is determined by the license(s) purchased. There is no limit to the number of individual users that can be protected on each PC.

With CyberPatrol Online Protection Pro, you can:

- Protect multiple computers and users from a single online location-the, Safety Center
- Access the Safety Center from any computer with an Internet connection
- Create separate protection levels for each user
- Receive threat alerts and reports sent directly to your e-mail

Product Applications

CyberPatrol Online Protection Pro offers six online safety applications, each of which can be turned off or on separately for each user.

Web Filtering	Filters and blocks bad and undesirable sites. Block adult material, illegal downloads and other unsuitable web sites.
Time Management	Controls times that individual users can spend online. Limit usage based on time of day or daily/weekly cumulative time allowances.
Safe Search	Monitors safe search features of Google, Yahoo, and Bing and assures they are set to highest safe searching level.
Sex Chat Alert	Monitors chat groups for sexually explicit conversations.
Harassment Alert	Monitors chats and alerts you of online communications that contain language often used to harass or bully someone.
Custom Alert	Monitors information, words, and numbers (credit card, SSN, phone numbers) that you select. You are alerted if any of the information is shared in chats.

Activating the Safety Center

There are two steps required to use CyberPatrol Online Protection Pro service;

1. Activate your Safety Center account
2. Install the Scanner on the computer(s) whose users you want to protect.

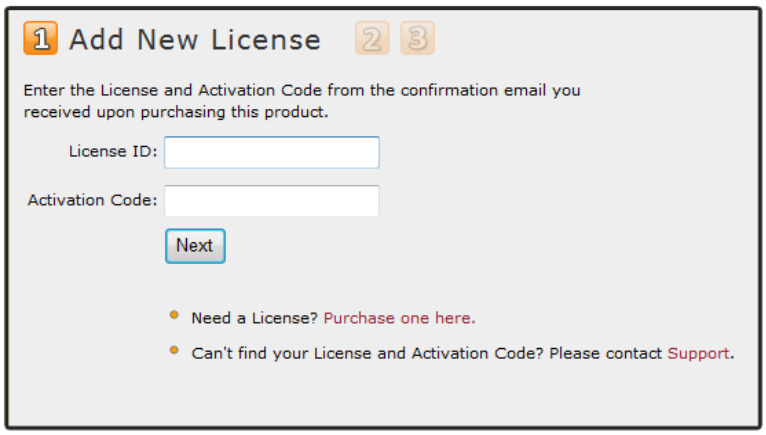
Activating Your Safety Center Account

Upon purchasing or trial of CyberPatrol Online Protection Pro, you will receive an e-mail that contains the following:

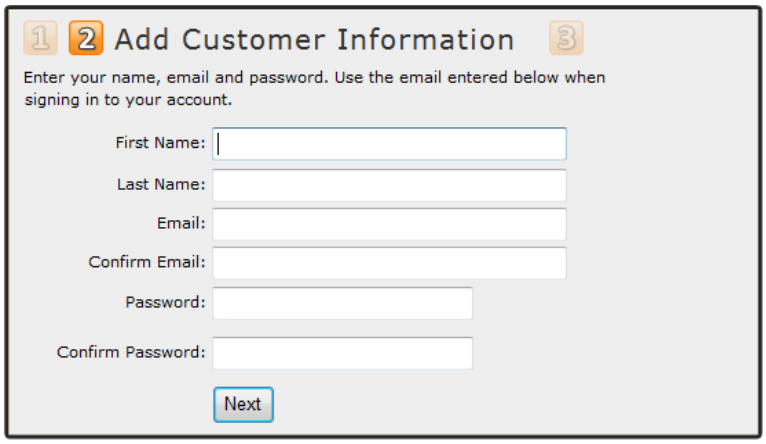
- Link to the activation site
- License ID
- Activation Code

1. To activate your account go to https://protectionpro.cyberpatrol.com/. The following screen will appear.

2. Click **Sign Up Now.** The Add New License Screen will appear. Enter the license ID and Activation Code you received via e-mail when you purchased the product.



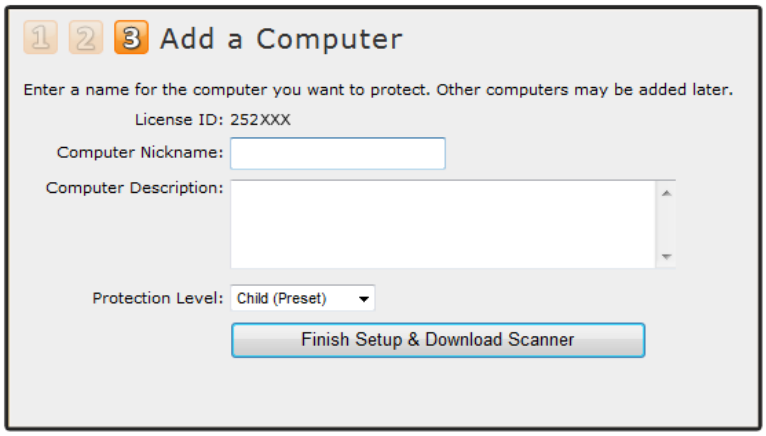
3. Click **Next**. The Add Your Customer Information Screen will appear.



4. Complete the required customer information fields. Your password must be at least 6 characters.

   Important: *You will need to use your password during set up and to manage your account. Please take the necessary steps to assure you don't lose your logon information.*

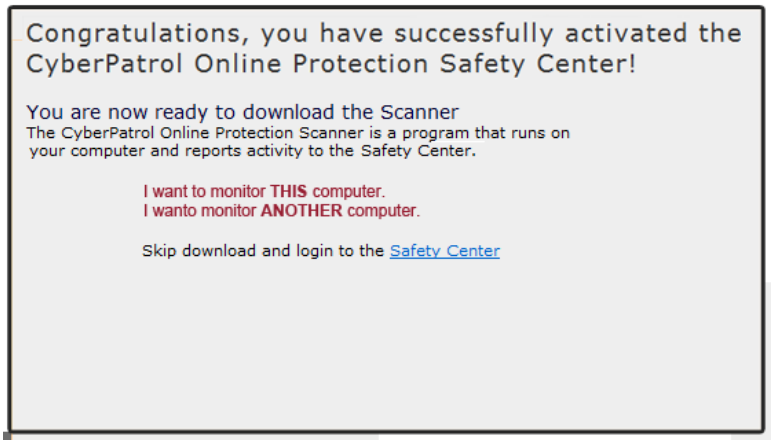
5. Click **Next**. The Name your Computer screen will appear:



6. Type in a name for the computer you want to protect like "Home Computer". If useful, you may also type in a computer description.

7. Select a default protection level for your computer. Choices are Manger1, Manager2, Employee1 and Employee2. Protection and monitoring options will be set based on your selection. You will be able to modify or customize selections anytime after installation is complete. If your computer has multiple user accounts, you can select different settings for each user **after** installation is complete.

8. Click **Next**. The Safety Center Activation is Complete screen will appear.



9. You will need to download the Scanner on the computer or computers you want to protect. If you are installing the scanner on this computer, Click "**I want to monitor THIS computer"**.

   If you are protecting another computer, access the internet from that PC and go to https://protection.cyberpatrol.com/downloads/OPClientSetup.exe.Install and set up the Scanner.

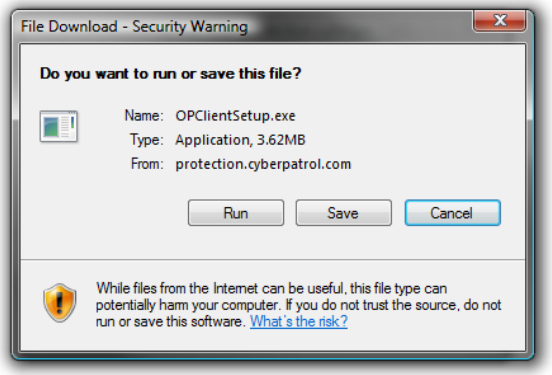
10. Click **Safety Center** to sign into the Safety Center or go to https://protection.cyberpatrol.com.

Installing and Using the Scanner

Scanner Installation

Once the Safety Center is setup, you will need to install the Scanner on the computer(s) you wish to protect.

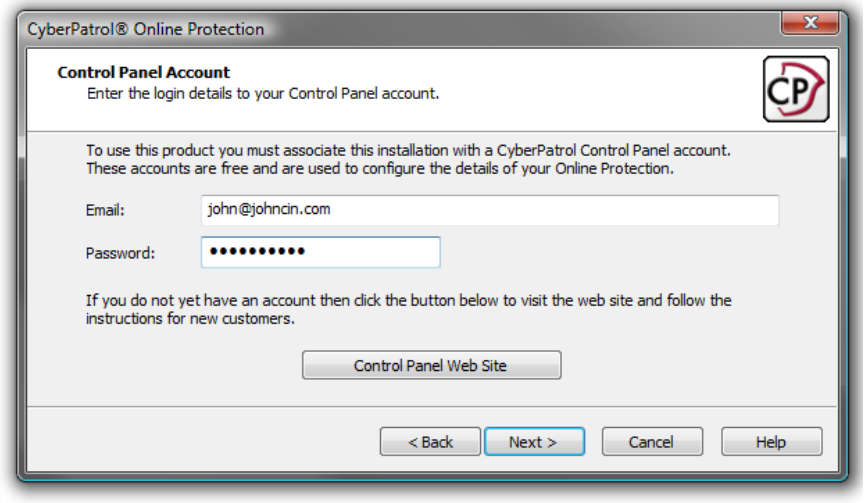
1. Download the software to the computer by going to https://protection.cyberpatrol.com/downloads/OPClientSetup.exe.The file download screen will appear. Click **Run** and the software will be downloaded to your computer.



2. Once the software download is complete, the CyberPatrol Online Protection Pro Setup Wizard will appear on your screen. Click **Next**.

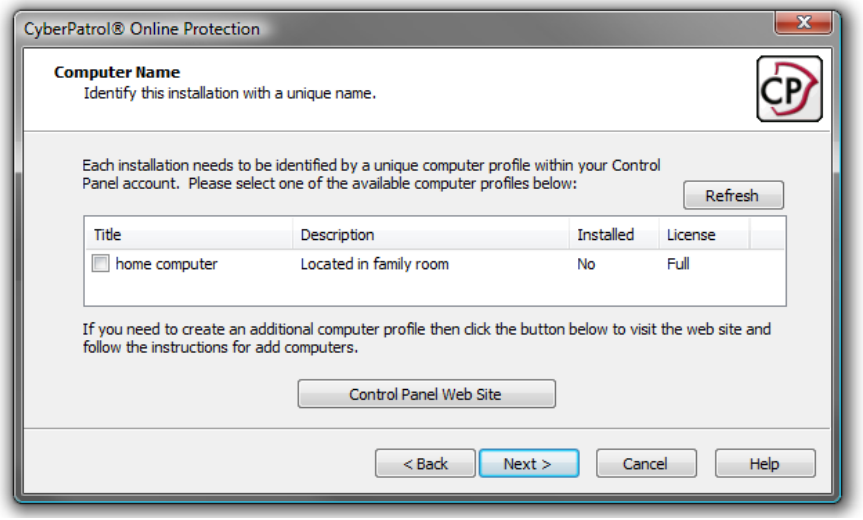
3. Follow the set up instructions. Upon completion, you will see a second setup wizard that will guide you through the steps for configuring CyberPatrol Online Protection Pro for your computer.

4. Click **Next**. The Safety Center Account Screen will appear.



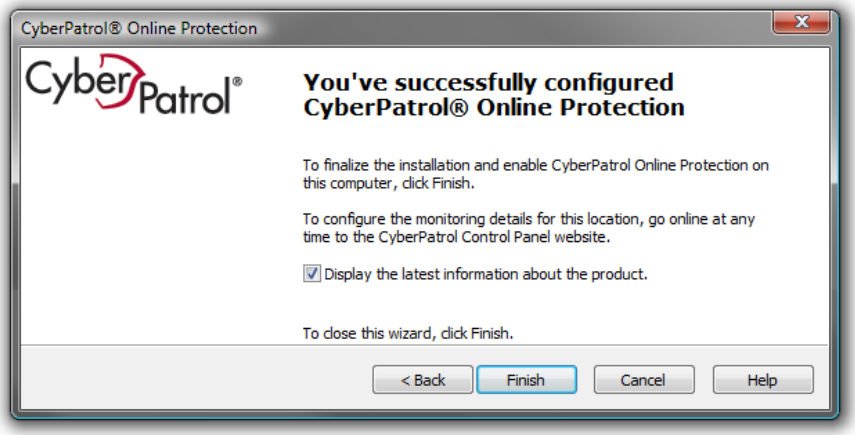
Enter the e-mail address and password that you used to activate your account. Click **Next**.

5. The following screen will appear.



6. Click the **Check Box** next to the computer that you are protecting. In most cases only a single computer is listed.

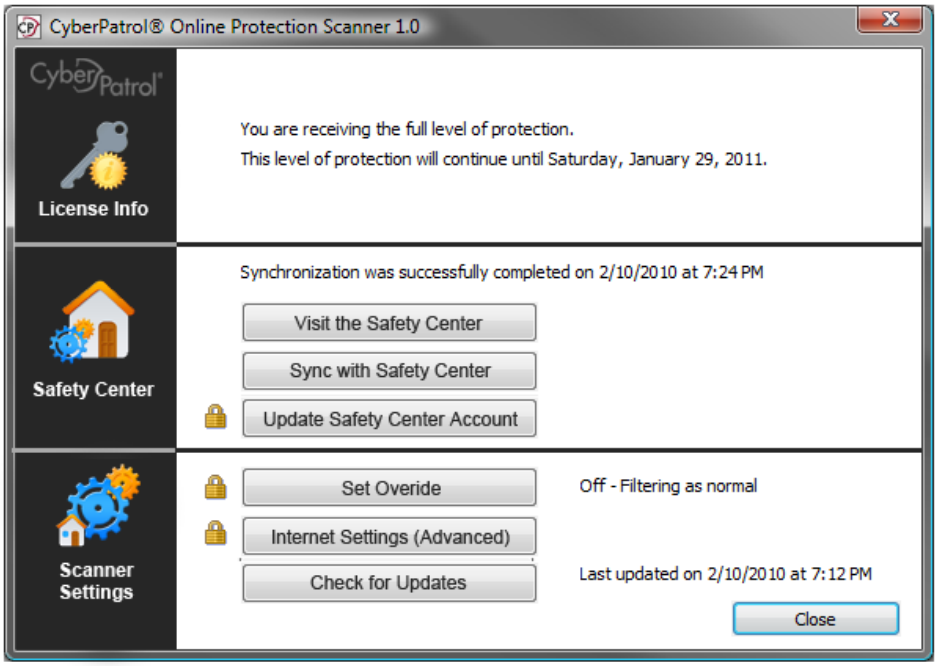
7. Click **Finish**. Your installation is complete and you are ready to begin using CyberPatrol Online Protection Pro.



Using the Scanner

The scanner is designed to run silently in the background in protected PCs. Once installed, you can access the scanner by clicking on the Scanner icon in the system tray.

The following screen will appear:



The main page of the Scanner is divided into three sections;

- **License Info** - Displays licensing information
- **Safety Center** – Synchronizes your scanner and allows interaction with the Safety Center
- **Scanner Settings** – Sets up the actions of the Scanner

Safety Center

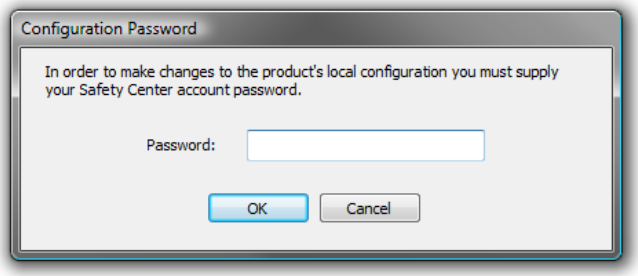
The Safety Center section displays the last time your Scanner updated information with the Safety Center. This process automatically takes place every few minutes. You can manually perform the operation by Clicking **Sync with the Safety Center**.

You can access the Safety Center from the Scanner by Clicking **Visit the Safety Center**.

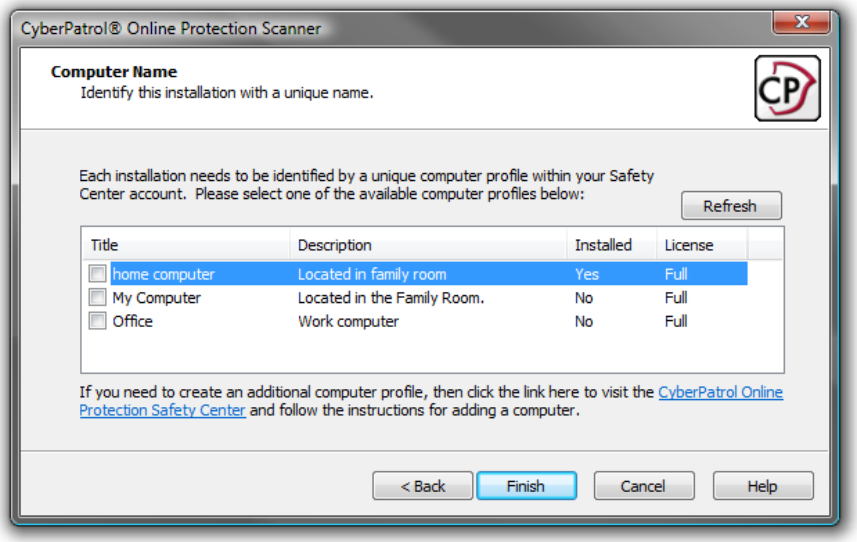
During installation, the scanner asked you to associate your Scanner with a computer name in the Safety Center. If you change your user name and or password, you will need to reestablish the connection between the Scanner and the Safety Center.

To sync the Scanner and Safety Center;

1. Click **Update Safety Center Account**. You will be asked to enter your Safety Center password.



2. You are then asked to enter your new email address (user name) and enter your new password. The following screen appears;



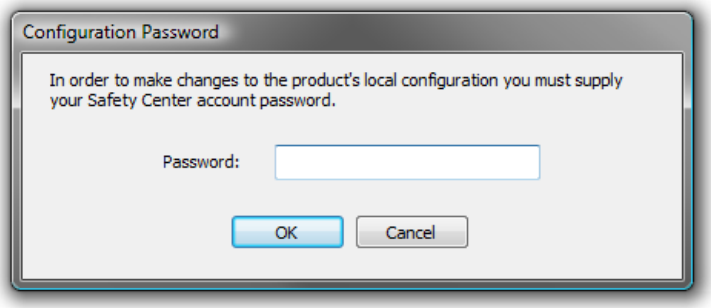
3. Check the box of the computer name that corresponds to the computer you are using.
4. Click **Finish**

Scanner Settings

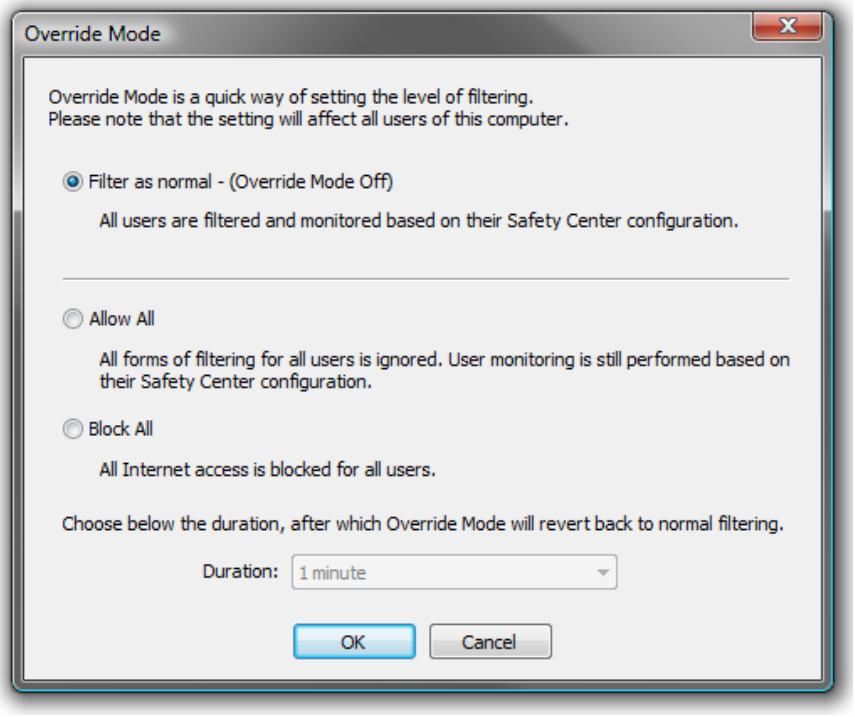
Scanner Settings lets you Set the Override Mode, Internet Settings, and check for Scanner Updates.

To change your override settings;

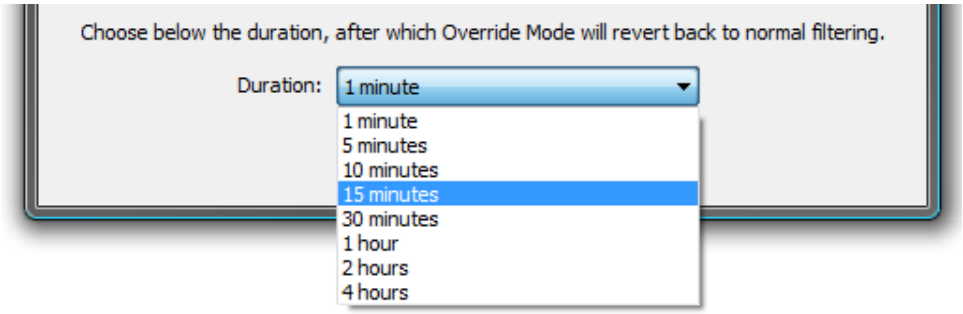
1. Click **Set Override.** You will be asked to enter your password.



2. Enter your password and Click OK. The following screen appears;

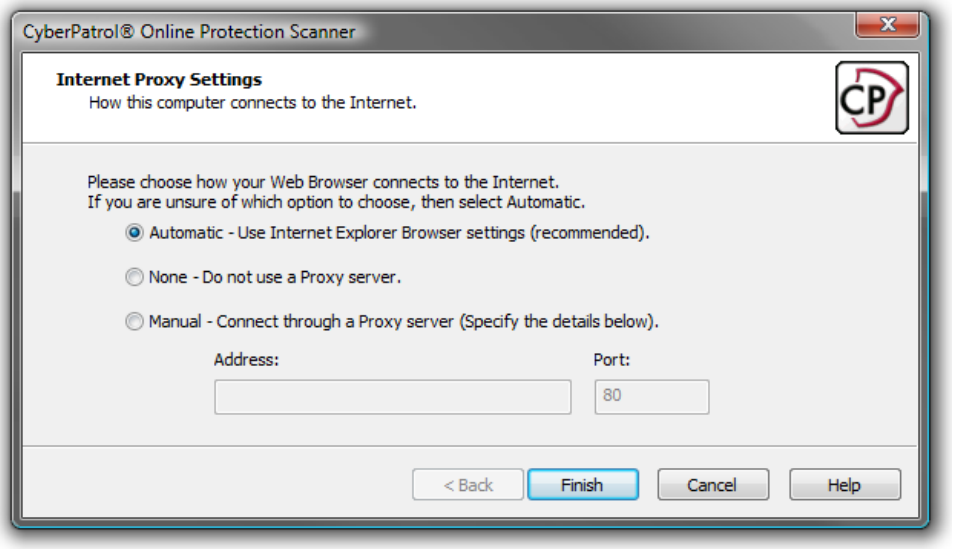


3. The normal mode is set to Override Mode Off. Click **Allow All or Block All** to change your settings.
4. Click the Duration **Drop Down Menu**.



5. Click the duration time for your setting.
6. Click **OK.** The Scanner will display a popup screen to let you know override has expired.

Internet settings are for advanced users and identify how your computer accesses the internet. These settings are automatically set. If you need to change Internet settings, Click **Change Internet Settings**. The following screen appears.



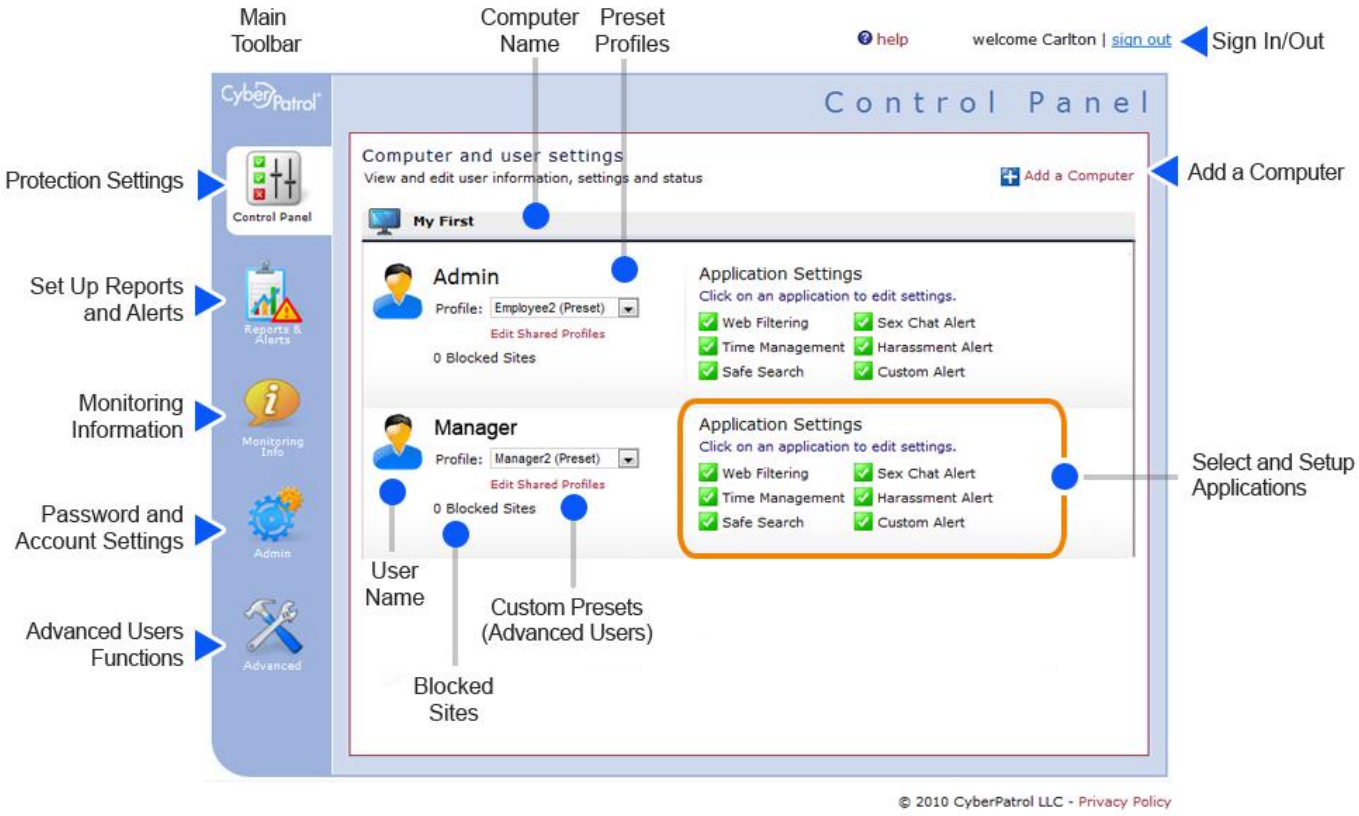
Select the proper settings and Click **Finish.**

Your software is automatically updated by CyberPatrol. If you want to assure that you have the latest updates, Click **Check for Updates.**

Safety Center Overview & Setup

Once you activate the Safety Center and install the Scanner on the appropriate PC, you are ready to select applications and safeguard levels for your computer and, if you want, individual users. CyberPatrol uses selectable preset levels for Manger1, Manager2, Employee1 and Employee2. Selecting a preset option will automatically set all filtering and alert levels.

You also have the option to create Shared Profiles with settings you select. Shared Profiles can be used with all users. You can modify any preset to refine the level of protection for a particular user. This creates a custom profile that is only available to that user.



Safety Center Site Control Panel

The Safety Center Control Panel is the primary control center for managing protection and alert settings. You can select computers to be protected and review or set both the kinds and levels of safeguards for each person using the PC. Computers are identified by the names assigned during activation.

Safety Center Site Control Panel

Main Toolbar	Navigate the five main sections of the Safety Center; Control Panel, Reports & Alerts, Monitoring Info, Admin, and Advanced.

Control Panel takes you to the main page for managing computer and user settings.
Reports & Alerts takes you to report and alert settings and information.
Monitoring Information helps you decide what to monitor and why,
Admin lets you manage computers, licenses and account information
Advanced takes you to advanced features; Shared Profiles and Add Users.

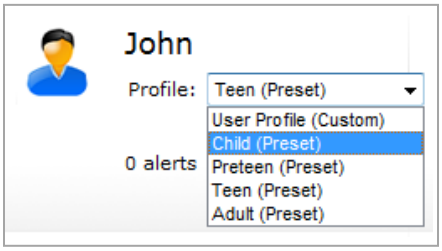
Add a Computer Used to add another computer to the Safety Center. Adding another computer may require purchasing an additional license.

Sign In/Out Used to sign in and sign out of the Safety Center.

Protected Computers Identifies each protected computer assigned to the Safety Center. The computer name is the name you assigned during account or license activation. Click on a computer name to manage or change settings for users of that computer.

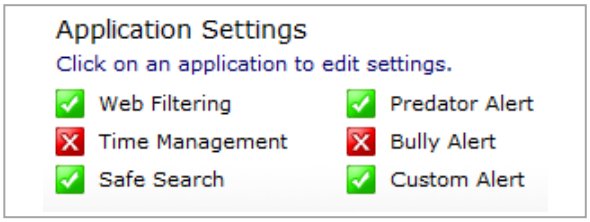
User Names Users are identified by the account names you created when you first installed and setup Windows on your PC. Additional users can be added to a computer by adding new user accounts to your Windows system.

Current Profile Indicates the current filtering and monitoring profile of a user. The profile is first selected during the installation process and can be changed by clicking on the drop down menu. There you can choose from one of four preset profiles or any Shared Profiles you may have created. *Profile options are: Child, Preteen, Teen, and Adult.*



Alerts Indicates the number of alerts sent for a particular user.

Application Settings Shows the current status of each application. A green check indicates on, a red X off.



To change the status of an application or modify its characteristics, click on the application name. Once on the application page, the application can be turned off or on by clicking the appropriate button next to the status indicator.

Each application page lets you select additional options depending on the function of the application. When prompted, you must Click **Save** for your changes to take effect.

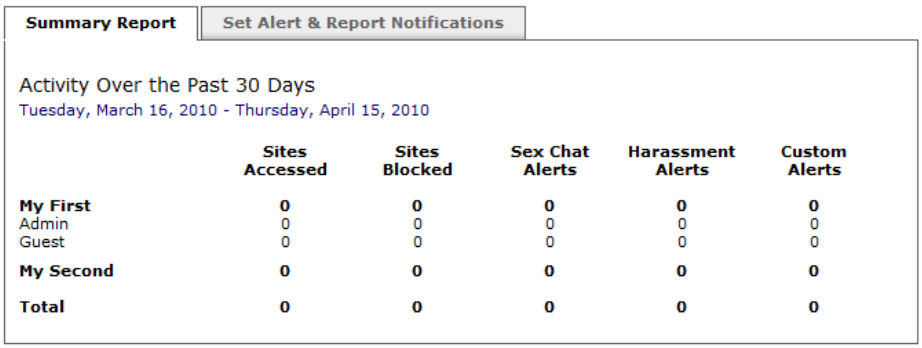
Edit Shared Profiles

Edit shared profiles is an advanced feature that lets you create or edit a profile that is available as a preset to all users. You create the profile name, select the applications that are turned on and off, and select the level of protection within each application.

Reports and Alerts

Reports and Alerts give you a summary report of all alerts, by computer and user that have been sent over the past 30 days. Reports are summarized by; Sites Accessed, Sites Blocked, Sex Chat Alerts, Harassment Alerts, and Custom Alerts.

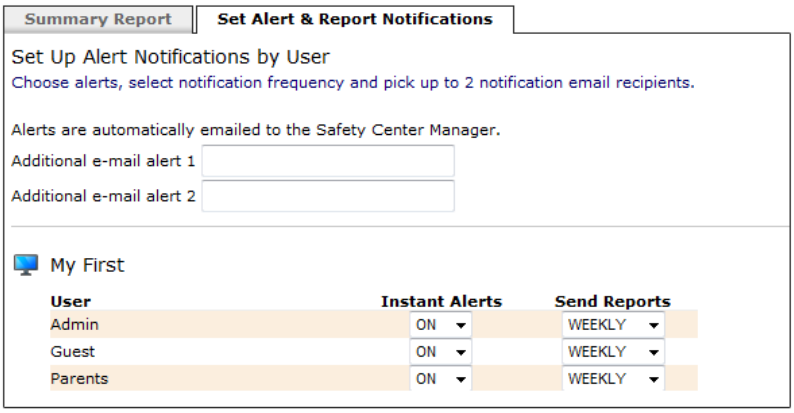
Summary Report



	Sites Accessed	Sites Blocked	Sex Chat Alerts	Harassment Alerts	Custom Alerts
My First	**0**	**0**	**0**	**0**	**0**
Admin	0	0	0	0	0
Guest	0	0	0	0	0
My Second	**0**	**0**	**0**	**0**	**0**
Total	**0**	**0**	**0**	**0**	**0**

Set Alert Notifications

There are two types of reporting in CyberPatrol Online Protection Pro; Alerts and Reports. Reports offer a summary of alerts, web site activity, and other events. An Alert is a notification sent by e-mail when a potential problem is identified. Both reports and alerts are automatically sent to the email account of the Safety Center Manager. Alerts are either Off or On and sent immediately. Reports are sent weekly or monthly.



You can identify two additional people to receive reports and alerts. Type their e-mail address in one of the Additional e-mail boxes under “Set Up Alert Notifications by User”.

Note: If you don’t receive alerts and are filtering mail, check your junk mail folder.

Alerts can be turned On or Off by user. Report frequency can be set to weekly or monthly by user. Click on the drop down menu; make your selection, and when prompted, Click **Save**.

Instant Alerts

If you have set Instant Alerts to **On,** you will be notified by e-mail whenever a Sex Chat, Harassment, or Custom alert is detected. The alert will contain detailed information about the incident. ***We do not store these reports nor do we keep the information reported to you.*** Once the alert is reported, all information is erased from our systems. If you want to maintain a log of alerts, we suggest that you save the information on your computer.

E-mails are sent from alerts@cyberpatrol.com. For security reasons, some information may be changed or disguised in the alert e-mail. We do not transmit sensitive information that could end up in the hands of others.

CyberPatrol Online Protection Alert
Generated: May 5, 2009 12:00:00 AM
Computer name: Bob's PC
User account: Bob
To change your alert settings or get more information about what actions to take in response to this alert, log on to https://protection.cyberpatrol.com

CyberPatrol® protecting people online

Alert Details - The following items are shown in the order they occurred. **Message**	**Time:** May 5, 2009 12:09:00 AM **To:** bobby **From:** katie **Subject:** Help me with my homework! **Body:** You had geometry already, right? **Incoming:** yes
Message	**Time:** May 5, 2009 12:09:00 AM **To:** katie **From:** bobby **Subject:** Help me with my homework! **Body:** You can get all of the answers on this site: www.homeworkcheats.com **Incoming:** no
Message	**Time:** May 5, 2009 12:09:00 AM **To:** bobby **From:** katie **Subject:** Help me with my homework! **Body:** Thanks. You should sneak out again tonight :-) **Incoming:** yes

Note: The events shown above triggered CyberPatrol Online Protection to send this alert. In some cases, a single event is enough to trigger an alert. In other cases, multiple events combine to trigger an alert. Some events may be included purely for the purpose of providing context.

Weekly or Monthly Reports

Depending on your selection, summary reports are sent weekly or monthly showing the number of blocks and alerts by user. Again, for security and privacy reasons, we do not store detailed alert information. Reports are sent from alerts@cyberpatrol.com.

Weekly or Monthly Reports

CyberPatrol Online Protection Weekly Report
Dates: 2/8/2010 12:00:00 AM - 2/14/2010 11:59:59 PM
Prepared for: Chris - e-mail

You can get reports at any time by logging on to https://protection.cyberpatrol.com

	Sites Accessed	Sites Blocked	Sex Chat Alerts	Harassment Alerts	Custom Alerts
Protected Computer1					
test	324	22	12	1	5

Last data reported on: February 15, 2010 7:54:01 AM

	Sites Accessed	Sites Blocked	Sex Chat Alerts	Harassment Alerts	Custom Alerts
Protected Computer2					
chris	301	2	1	44	7

Last data reported on: February 15, 2010 7:54:01 AM

Monitoring Info

The monitoring function within CyberPatrol lets you monitor chat activity by computer and individual user. Alerts are generated as a result of monitoring popular chat sites for trigger words or phrases. Three categories of chat are monitored; Harassment, Sex Chat, and Custom Terms. You select the type of alerts that you want to use.

The alert packages monitor popular chat programs and social networks looking for potentially harmful or risky activity. The monitoring function checks for incoming and outing instances of trigger words or phrases. Should an instance occur, the safety center manager is notified by e-mail.

Getting a single or several alerts does not necessarily mean that suspicious activity is taking place. However, if alerts are persistent and take place over an extended period of time, it's probably time to further examine the situation and take some action.

Monitored chat groups include:

- Windows Live Messenger
- Windows Messenger
- Yahoo Messenger
- Facebook IM
- MySpace IM
- Google Talk
- Psi
- Jabber/XMPP Clients

IMPORTANT NOTIFICATION

Cyber Patrol uses proprietary software to analyze communications and determine the possibility of inappropriate activity. While we do our very best to assure that all incidents of inappropriate communication are properly identified and that you are notified, the nature of this type of activity makes it impossible for any technology to be 100 percent accurate all of the time.

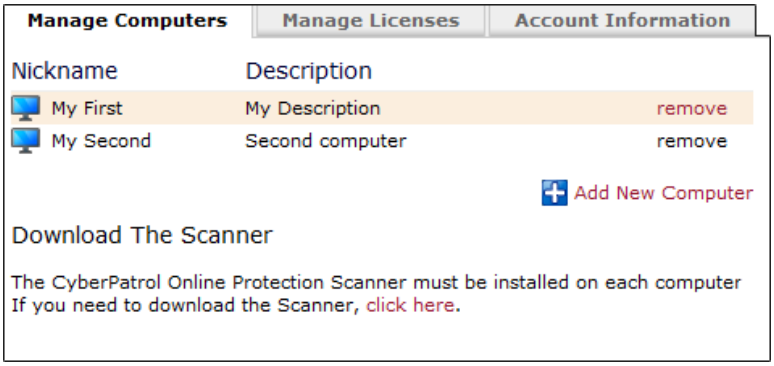
Admin

Admin lets you manage computers, licenses and your account information. You can add or delete protected computers, review and add licenses, change account information, and reset your password.

Manage Computers

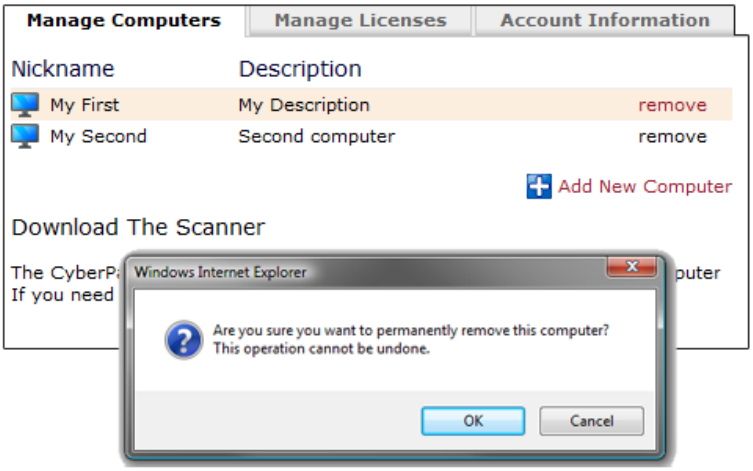
All computers, currently protected, are listed in this section by name and possibly with a description you created during set up. You can remove a computer in which case the software license becomes available for another PC.

This option also provides a link to the Scanner download.



To remove a computer;

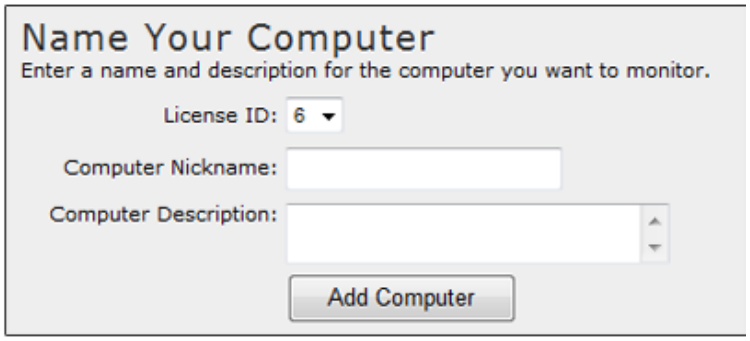
1. Click **Remove** next to the computer you want to delete. The following screen will appear asking if you are sure you want to remove the computer:



2. Click **OK.** The computer will be removed from the list and a notification will appear saying" Installation deleted successfully".

To add a computer:

1. Click **Add New Computer.** The Add a Computer screen will appear asking you to Name Your Computer.

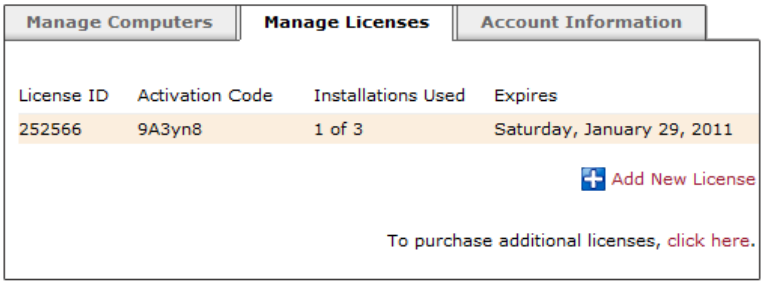


2. Use the drop down menu to select a license ID. If you do not have any available licenses, you will need to cancel the process and purchase an additional license before you can add a computer.
3. Type a name for the computer.
4. Optionally add a description

The Scanner must be installed on any computer that you want to protect. If you need to download the Scanner either Click **Click Here** or go to https://protection.cyberpatrol.com/downloads/OPClientSetup.exe. For further directions go the section titled *Installing the Scanner*.

Manage Licenses

This option identifies your current licenses, gives you the option to add new licenses, and provides a link to purchase additional licenses.

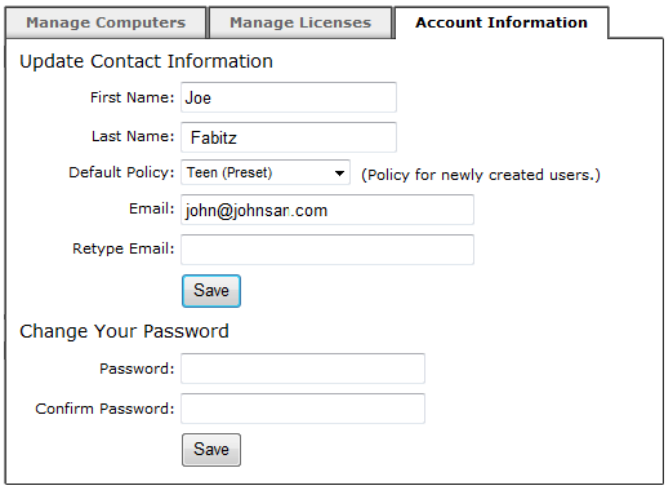


To add a new license:

1. Click **Add New Licenses**.
2. When prompted, enter your license ID and Activation Code
3. Click **Add License**. The license will be added to the list and a notification will appear saying “the license was successfully added”.

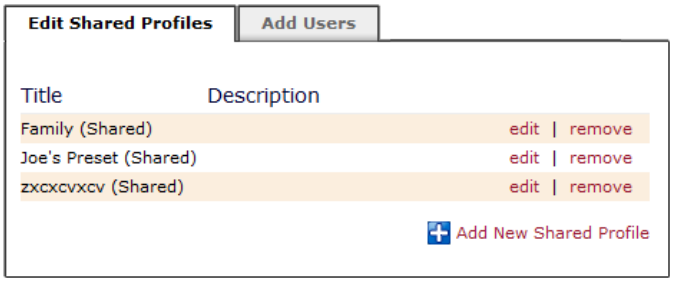
Account Information

This option lets you modify your contact information, select a new default policy, and change your password. Enter appropriate information as directed and Click **Save**.



Advanced

This option lets you modify the advanced features of CyberPatrol Online Protection Pro. You can Edit Shared Profiles and provide instructions for adding additional users to a protected PC.

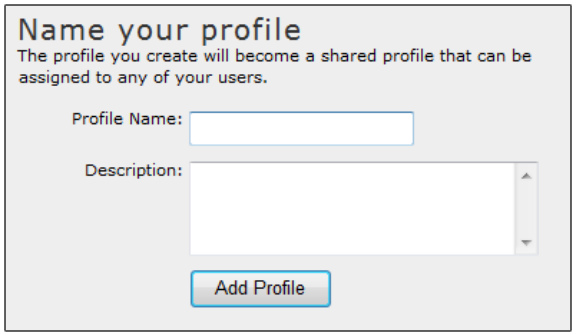


Edit Shared Profiles

A Shared Profile is one that can be shared across all users on all protected PCs. Just like the presets that come with the Safety Center, Shared profiles is a collection of settings that are applied to a user. Shared Profiles are identified and made available in the profile drop down menu. Each Shared Profile has a unique name that is assigned when created.

To add a Shared Profile:

1. Click on **Add a New Shared Profile.** The following screen will appear.



2. Enter a profile name and, optionally, a description of the profile.
3. Click **Add Profile.** Your profile is added to the list and a message is displayed that your profile was created successfully.

Now that a new Shared Profile has been named and added to the list, edit the profile to determine and select the settings for each application.

To edit a Shared Profile;

1. Click **Edit** next to the profile you wish to edit. A page, similar to the Control Panel, will appear with your Shared Profile name and the six applications displayed in the header.

2. Click on each application you want included in your profile and select any optional settings.
3. Once you have selected your options, Click **Save**.
4. Repeat this process for each application until you have made all of your selections.

Adding a User

CyberPatrol Online Protection Pro relies on the User Accounts in your Windows™ software to identify the Users on protected PCs. These users are typically setup when you installed Windows XP, Vista, or Windows 7. If you have previously set up individual user accounts they will be recognized by the Scanner and show up in the Safety Center. All computers have at least one user, the Administrator.

Adding additional users for Online Protection requires that you set up additional user accounts in Windows. Once a user is added to Windows, it will be detected by the Scanner and added to the user list in the Safety Center.

The process for setting up additional users is dependent on the version of Windows installed on your computer. To get detailed instructions on how to add a user, click on the name of the Windows software installed on the computer you are protecting.

Operating systems:

- Windows XP - support.microsoft.com/kb/279783
- Windows Vista - windows.microsoft.com/en-US/windows-vista/Create-a-user-account
- Windows 7 - windows.microsoft.com/en-us/Windows7/Create-a-user-account

Applications

CyberPatrol Online Protection Pro contains six applications; Web Filtering, Time Management, Safe Search, Harassment Alert, Sex Chat Alert, and Custom Alert. Web Filtering, Time Management and Custom Alert offer controls and settings that can be set and managed by the Safety Center Manager. The remaining three are either turned on or off.

The alert packages (Sex Chat, Harassment, and Custom) monitor popular chat programs and social networks looking for potentially harmful activity. You select the type of alerts that you want to use.

- **Sex Chat** - Monitors chat group conversations for sexually explicit conversations.
- **Harassment -** Monitors online chat that contain language often used to harass or bully someone.
- **Custom** - Monitors any name, phone number, address or words that you choose. If any custom entries show up in chats you are alerted.

In addition, some chat programs have the ability to send and receive encrypted (scrambled) messages. This can be an indication that something bad is being sent or received. Therefore, when the Safety Center detects an encrypted message, it immediately sends an alert.

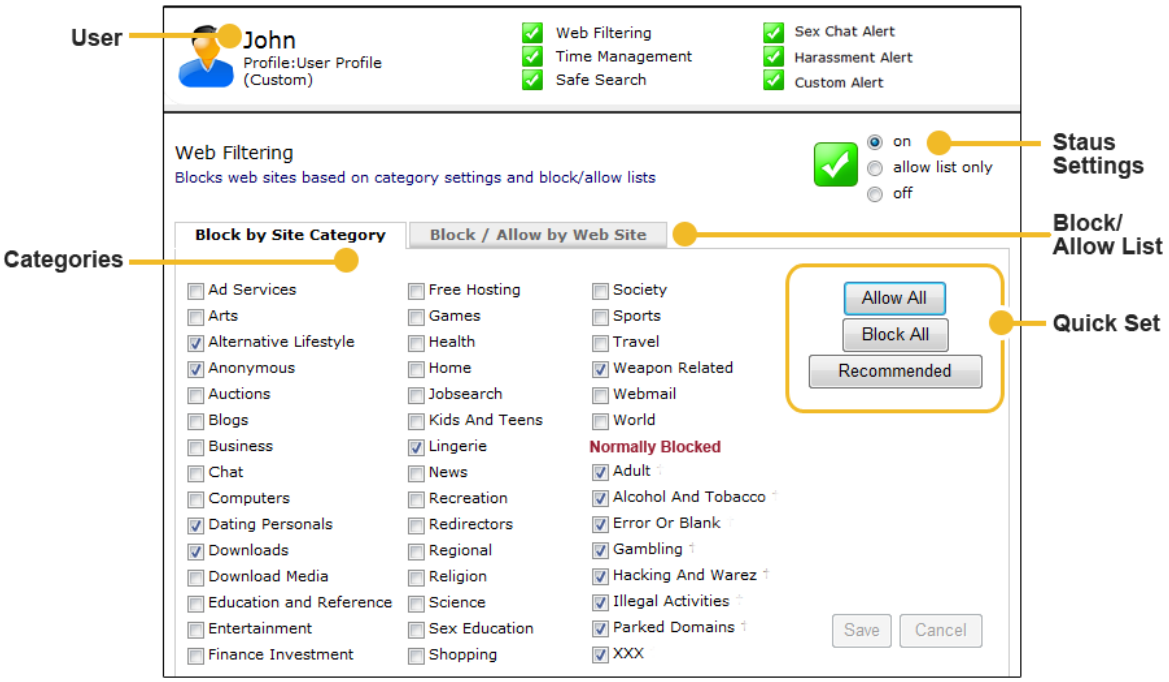
We monitor the online chat services listed below:

- Windows Live Messenger
- Windows Messenger
- Yahoo Messenger
- Facebook IM
- MySpace IM
- Google Talk
- Psi
- Jabber/XMPP Clients

Web Filtering

Web filtering is used to block access to web sites defined by the Safety Center Manager.

Web Filtering



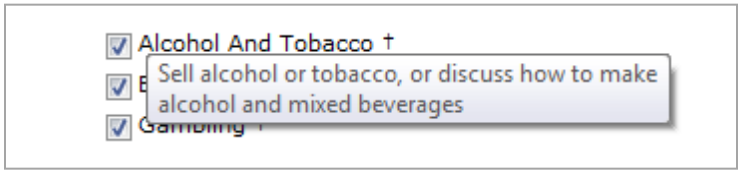
Web Filtering can be customized for each user. Initial Web Filtering settings are determined based on the Profile selected.

Web Filtering gives you three blocking options:

- *Block Sites by **Category & Allow List***
- *Block Sites Based on the **Allow List Only***
- *Turn Web Filtering Off*

Block by Categories
You can individually block categories of web sites. A check mark next to a category indicates that it is blocked.

Scroll your mouse over a category name to display a brief description of the kinds of web sites contained in that category. A complete description of categories is contained in the Additional Information section of this manual.



To add or remove a category from the blocked list:

1. Click the Block by Site Category tab. The following screen will appear.

2. Select the categories you want to block by Clicking on the box to the left of the category name to display a check mark. Repeat this process for all categories you want to select.

   Note: You can use the Quick Set buttons to Allow All, Block All, and Block Recommended. Click the appropriate quick set button.

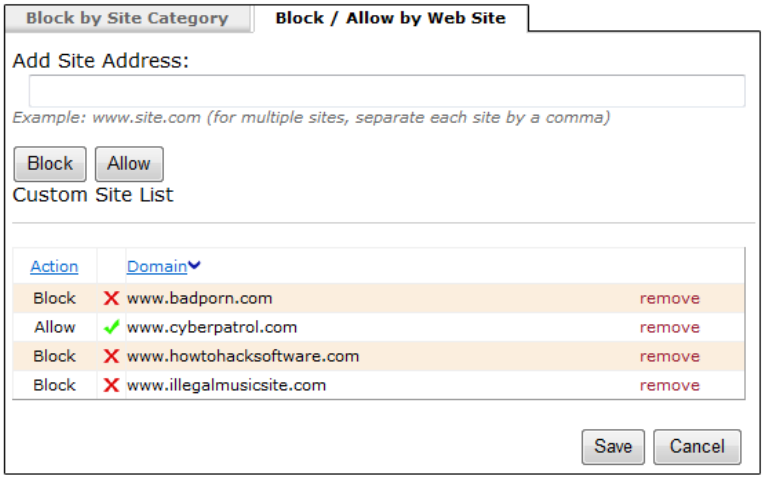
3. Click **Save**. Your changes are now in effect.

Block/Allow list

The Block/Allow List is made up of web sites that you want to always be blocked or allowed. Any site added to this list will override the settings in the blocked categories. If, for example, there are specific web sites you don't want users to visit, such as games or blog sites, you add the web address of that site to the list and indicate you want them blocked. Even though access to these sites is normally allowed, adding them to your Block/Allow list assures that they are always blocked.

To add a site or sites to the Block/Allow List:

1. Click the Block/Allow tab. The following screen will appear:

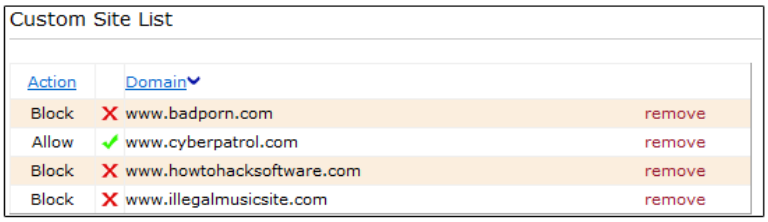


2. Click in the Add Site Address box and type the address of the Web site in the format: domainname.xxx (com, org, gov, etc.) ie facebook.com.

   Note: You can add multiple web sites by inserting commas to separate the list. Create a list of web sites in word or some other text editor separated by a comma. Copy the list and paste it into the Add Site Address box.

   (***Sample:*** www.testsite.com, www.mywebsite.com, www.another.com)

3. Click **Block** or **Allow** depending on how you want to always allow or block the web site. The web site will appear in the Custom Site list at the bottom of the page.



   Note: You can click on **Action** or **Domain** to display the list by action or in alphabetical order by domain name. Click **Remove** to remove an item from the list and then Click **Save**.

4. Click **Save**. The site is now added to your list.

Status Settings

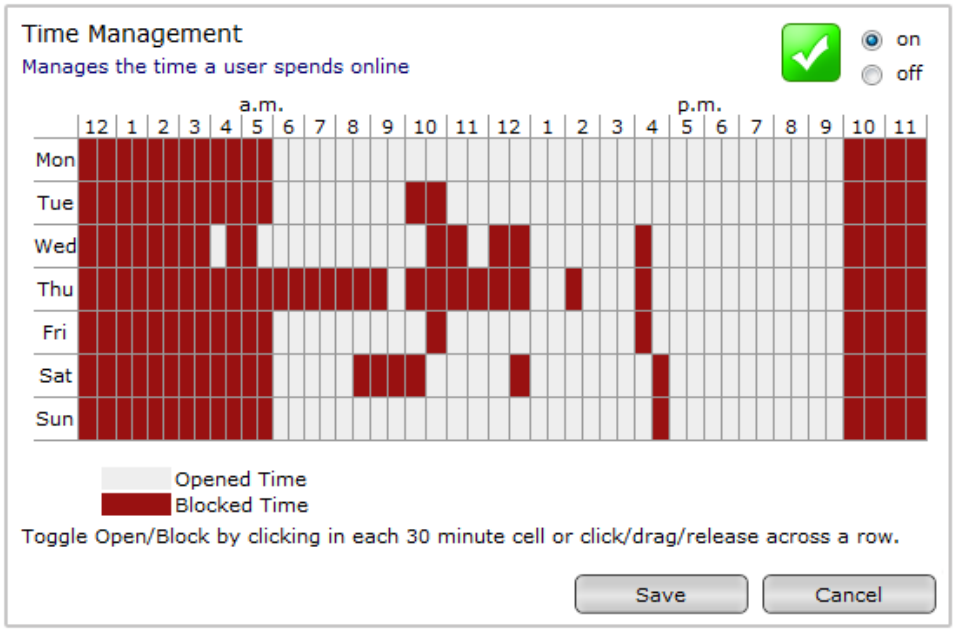
Web filtering can be turned off, turned on, or turned on with the Allow list only. If the status is set to on, both Category and Block/Allow functions are available. If the Status is set to Allow List only, only that function is available and category filtering is disabled.

Time Management

Time Management lets you control the amount of time a user can spend online. Access can be restricted by day of the week in half hour increments.

To use Time Management;

1. Click **on Time Management**. The following screen will appear.



   Make sure that the On /Off function is clicked to On.

2. Scroll over the time management grid to the date and time you want to control. Click your left mouse button to toggle the time off and on until it displays the setting you want.

   Note: Holding your left mouse down while scrolling lets you select multiple time blocks.

3. Click **Save**. Your new settings are now in effect.

SafeSearch

SafeSearch protects users by forcing SafeSearch to its strictest security settings in Google, Yahoo, and Bing. With SafeSearch turned off users are exposed to explicit images and content. This search engine feature blocks access to inappropriate content and images on these popular search engine sites. CyberPatrol Online Protection Pro prevents users from turning this feature off.

To activate SafeSearch,

1. Click the **ON** next to the red X button at the top right of the page.

2. Click **Save**. SafeSearch is now activated for the selected user.

Sex Chat Alert

Sex Chat Alert scans for any sexually explicit content, it reports all instances regardless of the source. That includes chat between consenting people.

To activate Sex Chat Alert,

1. Click the **ON** next to the red X button at the top right of the page.

2. Click **Save**. Sex Chat Alert is now activated for the selected user.

Harassment Alert

Harassment Alert monitors chat for harassing chat and terms commonly used by bullies. Since Harassment Alert scans for common bully terms it reports all instances regardless of the source.

To activate Harassment Alert,

1. Click the **ON** next to the red X button at the top right of the page.

2. Click **Save**. Harassment Alert is now activated for the selected user.

Custom Alert

Custom Alert lets you enter phone numbers, names, addresses, and other information that you want to monitor in social networking and other chat sessions. You can choose from pre-defined formats or create generic text. Anytime an item you have entered is used in a chat session, you are alerted.

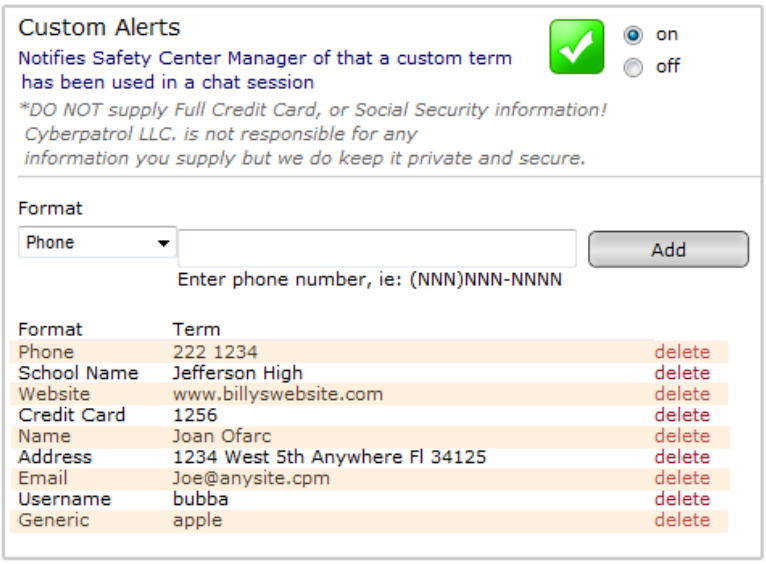
Important: When entering information in the Generic format, be careful not to use commonly used terms like "the". Doing so will generate a large number of false alarms.

Pre-Defined formats include:

- Phone
- School Name
- Website
- Credit Card (only the last four numbers)
- Name
- Social Security numbers (only last four numbers)
- Address
- Email
- Username
- Generic

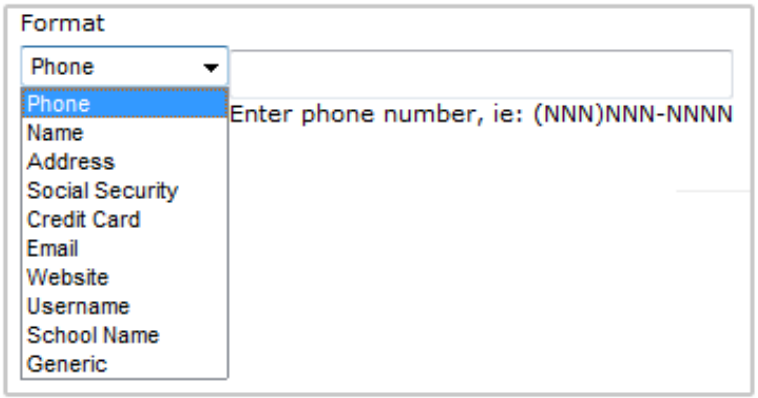
To create Custom Alerts:

1. Click on **Custom Alerts**. The following screen will appear.



Make sure that the On/Off function is clicked to On.

2. Click the Format drop down menu to select the format of the information you want to enter. The following screen will appear:



3. Click the format you want to use and enter the information as directed. Click **Add**. The new item will appear in the list of custom terms.

Format	Term	
Phone	222 1234	delete
School Name	Jefferson High	delete
Website	www.billyswebsite.com	delete
Credit Card	1256	delete
Name	Joan Ofarc	delete
Address	1234 West 5th Anywhere Fl 34125	delete
Email	Joe@anysite.cpm	delete
Username	bubba	delete
Generic	apple	delete

Note: You can delete any item on the list by clicking delete next to the item you want to remove.

4. Click **Save**. Your new settings are now in effect.

Additional Information

System Requirements

CyberPatrol Online Protection Pro is designed for Windows-based standalone PCs. It is also used for small networks of server-based PCs, by installing and licensing CyberPatrol Online Protection Pro on each PC to be filtered.

Microsoft® Operating Systems:	• Windows® 7 • Windows® Vista SP1 + • Windows® XP Home & Pro SP2 * + • Windows® 2000 Professional SP3 +
Processor:	Pentium II or higher
Memory:	512 MB minimum
Disk Space:	100 MB
Internet Browsers:	• Microsoft® Internet Explorer 7.0 and above • Mozilla Firefox 3.0 and above • Google Chrome 3.0 and above • AOL 8.0 and AOL 9.0
Internet Connection:	A valid Internet connection is required.

Notes:

* With Microsoft® Internet Explorer 7.0 or above installed.
- We recommend you have the latest Microsoft® security patches installed.
- Support is only for 32-bit operating systems.

Uninstalling CyberPatrol Online Protection Pro

To uninstall CyberPatrol Online Protection Pro use the standard approach for removing programs from your computer using the Windows Control Panel area. Click On CyberPatrol Online Protection Pro and select uninstall. During the uninstall procedure, you may be asked to supply your CyberPatrol Control Panel account password. If however your password is not being accepted, please contact CyberPatrol support.

Web Filtering Categories and Definitions

Web filtering is divided into two major types; normally blocked and normally allowed. Normally blocked categories are those that are typically deemed as inappropriate for under age users.

Typically Blocked Categories

Adult	Sites that discuss adult topics, phone sex, adult chat rooms. Nudity may be included, but not graphic sexual content. Hate, advocating of violence, Satanism and other subversive groups are included. Domains that sell adult novelty items (vibrators, and sex toys), or adult videos.
Alcohol and Tobacco	Sites that sell alcohol or tobacco, or discuss how to make alcohol and mixed beverages.
Error or Blank	Domains that either do not resolve to a valid server, or are misconfigured.
Gambling	Online gambling, bookmaking, sports betting, dog tracks, horse race betting. Sites that host gambling events but do not allow online betting are not included.
Hacking and Warez	Sites that discuss or distribute tools for hacking, cracking, attacking, or phreaking systems. Any site that contains keys, serial numbers, or cracked downloads for pirated programs.
Illegal Activities	Illegal online pharmacies (prescription free purchasing), how to modify weapons, bomb making, phishing, credit card fraud, illegal drugs and drug manufacturing, or recreational drug usage.
Parked Domains	Domains that are parked. These include companies like Seeq.com and others who hold domains and pay people for their usage.
XXX	Graphic adult material. Pornographic sites and sites that sell pornographic material.

Normally Allowed Categories

Ad Servers	Companies that serve or provide banner or other types of advertising.
Alternative Life Style	Gay, Lesbian, Nudist Colony, etc. No nudity may be expressed on the site. These sites talk about these alternative lifestyles only.
Anonymizers	Attempt to bypass Internet filters or provide information about how to do it. May include systems to make your Internet connection anonymous or hide your identity.
Arts	Museums, art galleries, artist sites, photographers. Artistic nudes may appear.
Auctions	Allow auctions and/or bidding on their site.
Blogs	Either offer blogging service or personal pages for individuals or families.

Business	Run by a business. They may or may not be trying to sell something. If they are trying to sell something online they will also be put in the shopping category.
Chat	Contain a chat area or are primarily dedicated to online chat.
Computers	Computer related sites. May discuss computer software, programming, how to repair them, etc. Computer companies will also be listed here. Sites that offer downloads of products will also be listed in the downloads category.
Dating and Personals	Online dating guides and matchmaking services.
Download Media	Music, streaming radio, movie trailers or any other media type of download.
Downloads	If there is any type of application available for download from a site it will be in this category. Sites that specialize in downloads (like download.com) are in this category. Sites that offer downloadable music are also in this category.
Education and Reference	Schools, universities, and sites that are primarily dedicated to research for schools. Online homework help sites are included in this category.
Entertainment	Sites that include information about the entertainment industry, or are for personal entertainment. Movies, television, and magazines are included here. Joke sites and other online gaming sites may be included here. Games are also included in the game category.
Finance and Investment	Any site that offers stock trading, investment advice, or online banking.
Free Hosting	Companies that allow free webpage hosting. If they have a canonical name for their free hosting only that is entered.
Games	Gaming sites, and gaming related activities sites. Gambling related sites are not included here. Casino and other online betting are in the blacklist for gambling. Poker and other gambling games (that do not allow betting) may be included here.
Health	Health related sites that are legal in nature. Hospitals, and medical related sites like legitimate pharmacies. Online pill sites are classified in the blacklist for illegal activities.
Home	Home decorating, appliances and things that are purchased for homes. Real estate for homes is also in this category.
Job Search	Resume posting and job hunting sites.
Kids and Teens	Sites appropriate for children and teens. Some teen online help sites are included.
Lingerie	Sell or promote lingerie. No graphic photos allowed.
News	News agencies and outlets. This includes press release sites.
Recreation	Recreational activities (Canoeing, hiking, boating, sailing, skating, weightlifting). Includes both outdoor and indoor recreation. Sports is found in a separate category.
Redirectors	Primary purpose to redirect you to another site. This may be to hide the identity of the destination site. Tinyurl.com is an example.
Regional	City, state, country, military, or government sites.
Religion	Religious discussion sites, and sites for churches. No hate or pro violent religious sites allowed.
Science	Science and discussions of science related information. Biology, DNA, and science related companies (Science labs).

Sex Education	Sexual education and additional sites. No graphic adult material allowed.
Shopping	Offer something for sale on their site.
Society	Clubs, organizations for causes (non profits), social issues like politics.
Sports	College, amateur, professional, and Olympic sporting events and activities. Sporting equipment sites are also included here. Locations that primarily offer sporting activities are included (bowling alleys, gyms, etc).
Travel	Travel agents, destinations or companies who specialize in travel services.
Weapon Related	Weapon related sites for guns and knives that are not illegal. Gun clubs, hunting, legal weapon sales, etc.
Web Mail	Offer webmail from their domain.
World	Domains here may be in some categories above if they have an English speaking page. No graphic sites are in this category. If a domain contains no English it will be classified here.

Definitions and Terminology

The following terms are used to describe functions and applications within CyberPatrol Online Protection Pro

Online Protection	The name of the complete CyberPatrol product including the Safety Center web site and the Scanner software that runs on protected computers.
Application	Refers to the individual applications that run within the Safety Center. There are currently 6 apps: Web Filtering, Time Management, SafeSearch, Harassment Alert, Sex Chat Alert, and Custom Alert.
Safety Center	This term refers to the product web site from which Safety Center Managers can control and administer all applications, alerts, reports for any computer running the scanner.
Safety Center Manager	The person who owns the product license and controls Safety Center settings.
User	A person that is identified as the user of any protected PC.
Scanner	The software that runs all protected PCs.
Profile	Identifies the level of protection for a user.
Preset Profiles	There are 4 preset profiles; Child, Pre-Teen, Teen and Adult.
Custom Profile	Any profile created specifically for a particular user. Each custom profile is specific to that user.
Shared Profile	A profile created by the Safety Center Manager that can be shared across all users on all protected PCs. Each Shared Profile has a unique name that is assigned when the profile is created.
Report	A summary of alerts, web site activity, and other events.
Alert	A notification sent to the Safety Center Manager when a potential problem is identified.